Patrick L. Oot, Jr. (admitted *pro hac vice*)
SHOOK, HARDY & BACON L.L.P.
1155 F Street, N.W., Suite 200
Washington, D.C. 20004
Telephone: 202.783.8400
Facsimile: 202.783.4211
Email: oot@shb.com

John K. Sherk (SBN 295838)
M. Kevin Underhill (SBN 208211)
Elizabeth A. Lee (SBN 312957)
SHOOK, HARDY & BACON L.L.P.
One Montgomery, Suite 2700
San Francisco, CA 94104
Telephone: 415.544.1900
Facsimile: 415.391.0281
Email: jsherk@shb.com
Email: kunderhill@shb.com

Attorneys for Defendants
UBER TECHNOLOGIES, INC.;
UBER USA, LLC; and RASIER-CA

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MICHAEL GONZALES, individually and on behalf of all other similarly situated,

Plaintiff,

v.

UBER TECHNOLOGIES, INC.; UBER USA, LLC; RASIER-CA, and DOES 1-10, inclusive,

Defendants.

Case No. 3:17-cv-02264-JSC

DEFENDANTS' MOTION TO DISMISS PLAINTIFF'S SECOND AMENDED COMPLAINT

Date: September 20, 2018
Time: 9:00 a.m.
Dept.: Courtroom F – 15th Floor
Judge: Hon. Jacqueline Scott Corley

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

In most ways, Plaintiff's third effort is not significantly different from the second (or the first). It is still based mainly on an article Plaintiff read online. It is still conclusory. And though this case is supposedly about egregious conduct that seriously harmed former Lyft driver Michael Gonzales, like the first two complaints this one says virtually nothing about him. Was he harmed? How does he *know* he was harmed? Why did he stop using the Lyft app (almost four years ago)? Does he have any intent to start again? If not, how could he be harmed today even if Uber still had data it collected about his location in 2014? And how could that harm be so serious today that it rises to the level of a state constitutional violation? The Second Amended Complaint still does not answer any of the questions above, nor does it fix the problems the Court identified last time around.

First, it does not fix the problems the Court identified with the UCL claim. With regard to injunctive relief, Plaintiff does *not* allege that he intends to start driving for Lyft again. He alleges only that he "may," which does not state a claim. And because Plaintiff's allegations about monetary relief are unchanged, that part of the UCL claim also fails. There is nothing left of it.

Second, the SAC does not fix the Stored Communications Act claim because Plaintiff has again failed to allege that Uber accessed communications in "electronic storage." Plaintiff now claims only that the communications were being stored "for purposes of backup protection," but alleges nothing to support that. To the contrary, he alleges the communications were stored for "liability purposes," or for Lyft's own business purposes, but alleges no facts suggesting backup protection. For that matter, there cannot be a "backup" copy unless there were at least two copies to start with. Here, Plaintiff alleges only one: the data Lyft was storing. The SCA does not apply.

Third, the problem with the California Data Access and Fraud Act claim last time was that Plaintiff had not alleged facts explaining the violation; he just parroted the language of the statute. Little has changed. Plaintiff's claim now appears to be only that Uber "accessed" data that he personally owned, citing his contract with Lyft. But he does not explain just what data was his exclusively, if any, or why or how that contract establishes that CDAFA applies.

Finally, most of the changes to the SAC deal with Plaintiff's argument that the U.S. Supreme Court's recent decision in *Carpenter v. United States* rescues his California state constitutional

claim. But *Carpenter* was a narrow ruling in a federal criminal case, holding only that, because of Fourth Amendment concerns about arbitrary government power, the government has to get a warrant if it wants to rummage through wireless carriers' records of cell-site location information. The Court specifically held that it was not otherwise disturbing the established principle that a party generally has no reasonable expectation of privacy in information he or she hands over to third parties. Nor is the conduct alleged here anything like the pervasive surveillance about which the Court was concerned in *Carpenter*. Plaintiff has not shown and cannot show that *Carpenter* applies here. Even if he could, that would not fix the other problems the Court identified—among them the problem of identifying "serious harm" to Michael Gonzales, or anyone else, as a result of Uber's alleged collection of limited location data Lyft drivers contractually agreed to give Lyft, in an effort to identify (and give bonuses to) "dual-app" drivers.

Because Plaintiff has not addressed the problems this Court identified when it dismissed the FAC, and for the other reasons above, the Court should dismiss the case with prejudice.

BACKGROUND AND NEWLY ALLEGED FACTS

- **Plaintiff's first two complaints**

Plaintiff's initial complaint, filed in April 2017, was based almost exclusively on an article that appeared on *The Information*, a website that covers the tech industry. *See* Compl. (Doc. 1). Of the six pages of substantive allegations, four of them were comprised of that article (verbatim) and excerpts from a *Washington Post* article based on it. *Id.* at pp. 7–12. Plaintiff alleged claims under the Wiretap Act, the state equivalent (CIPA), the UCL, and California's constitution. After a round of briefing, the Court dismissed that complaint with leave to amend. Order Granting Motion to Dismiss (Doc. 27) (Aug. 31, 2017).

Plaintiff filed an amended complaint in September 2017. First Am. Compl. (Doc. 34). He added claims under the Stored Communications Act and California's Computer Data Access and Fraud Act, but the FAC was still based mainly on the previously cited article, as well as more than three dozen allegations made on "information and belief." *See* Uber's Mot. to Dismiss FAC (Doc. 38) at 1:26–2:9 (citing these allegations). After a second round of briefing, the Court again dismissed

the complaint, this time issuing detailed orders. *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078 (N.D. Cal. 2018); *on reconsideration* 2018 WL 3068248 (N.D. Cal. June 21, 2018).

- **The Court's orders dismissing the First Amended Complaint**

The Court dismissed the Wiretap Act and CIPA claims for similar reasons: Plaintiff did not allege Uber "intercepted" the "contents" of a communication or that it had "eavesdropped" on one. 305 F. Supp. 3d at 1084–87, 1088–90. The CIPA claim under section 637.7 also failed, the Court held, because Plaintiff had "consented to the tracking of his vehicle through his cellphone when he signed up to be a Lyft driver." *Id*. at 1090. The Court dismissed that claim without leave to amend. It granted leave to amend the Wiretap Act claim, "but only to the extent Plaintiff can allege *consistent with Rule 11* that Uber intercepted the content of a communication from Plaintiff." *Id*. at 1087 (emphasis added). Instead, Plaintiff has dropped the Wiretap Act and CIPA claims entirely.

The Court held that the Stored Communications Act claim failed because Plaintiff had not "alleged facts that plausibly suggest that the communications were in 'electronic storage'; that is, that the communications were temporary or were in storage for the purpose of backup protection." 305 F. Supp. 3d at 1087. Plaintiff himself alleged that the communications were stored permanently, not temporarily, and Plaintiff admitted he had pleaded no facts showing Lyft stored the relevant information for backup purposes. *Id*. at 1087–88. The Court granted leave to amend "to allege facts that show Uber accessed communications in 'electronic storage.'" *Id*. at 1088.

Plaintiff's CDAFA allegations were no more than "boilerplate" that "parrot[ed] the language" of the statute, leaving Uber and the Court to "guess how Plaintiff contends these subsections were violated." 305 F. Supp. 3d at 1090. Further, the Court noted that the statute requires plaintiff to "allege that Uber accessed *Plaintiff's* computer, computer system, etc.," not Lyft's. *Id*. The Court granted leave to amend "to the extent Plaintiff can allege facts that plausibly suggest Uber violated a particular subsection of the Act." *Id*. at 1091.

As for Plaintiff's claim under the California Constitution, the Court held that he had not adequately alleged any of the three required elements. First, while he had sufficiently pleaded a "protected privacy interest" as to home addresses and "arguably precise geolocation data," the Court rejected his argument that the other information Uber allegedly obtained—his name, Lyft ID

number, and the implied message that he was "working as a Lyft driver"—were protected. 305 F. Supp. 3d at 1091. Second, the Court found Plaintiff had not alleged a reasonable expectation of privacy, given that he had "consented to the sharing of his geolocation data with perfect strangers" to work as a Lyft driver. *Id*. at 1091–92. This was true even if the data might reveal his home address, the Court held, because users of an app like Lyft's "cannot reasonably expect that this information will remain private." *Id*. at 1092. Third, even if Uber had obtained Plaintiff's name and home address, this did not allege a "serious" or "egregious" invasion of privacy "[w]ithout more allegations as to what, if anything, Uber did with this information...." *Id*. at 1093.

On reconsideration, the Court held Plaintiff had not adequately alleged a UCL claim. *Gonzales v. Uber Techs., Inc.*, No. 17-cv-02264-JSC, 2018 WL 3068248, at *3 (N.D. Cal. June 21, 2018). Plaintiff's allegations that Uber used its program to harm Lyft or "decrease[ ] the effectiveness of the Lyft app," which in turn allegedly harmed Plaintiff, were allegations of "classic money damages, not restitution," and therefore could not support recovery under the UCL. *Id*. at *2. Nor had Plaintiff alleged grounds for injunctive relief. *Id*. at *1–2. He stopped driving for Lyft in November 2014, did not allege Uber's program lasted beyond 2016, and did not allege any intent to drive for Lyft in the future. *Id*. at *2. He therefore had alleged no facts showing it was plausible that Uber would either use his more than three-year-old geolocation history to his detriment or that he would be harmed if Uber restarted its program. *Id*. Again, the Court granted leave to amend.

- **Plaintiff's Second Amended Complaint**

Plaintiff filed the current complaint on July 18. Second Am. Compl. (Doc. 58.). As noted, Plaintiff has dropped the Wiretap Act and CIPA claims. The attached comparison of the FAC and SAC shows that the changes are not extensive. *See* Ex. A.[1] In fact, in only a few places are the changes anything more than trivial:

- Plaintiff now argues he only "licenses" his "personal data" to Lyft and continues to "retain full ownership" of it. SAC ¶¶ 5, 135, 143.
- Two new paragraphs describe Plaintiff's claim that Lyft retains the information "for backup purposes." SAC ¶¶ 57, 133.

[1] This is the second time Plaintiff has failed to comply with the Court's standing order requiring a comparison to be filed along with any amended pleading. *See* Civil Standing Order at 3.

- A few new paragraphs attempt to further distinguish between what prospective riders might see on the app and what Uber supposedly collected. SAC ¶¶ 74–83.
- Plaintiff adds an argument that Uber's alleged program affected "surge pricing" or what Lyft apparently calls "Prime Time." SAC ¶¶ 101–06.
- Plaintiff says some rides he accepted were cancelled and suggests it is "plausible" the cancellations were because of Uber's program. SAC ¶¶ 126, 154–55.
- By far, however, the most significant additions to the SAC involve Plaintiff's effort to analogize this case to *Carpenter*. SAC ¶¶ 13, 115–16, 161–80.

As discussed below, most of this is not material, and none of it is sufficient to fix the problems the Court identified in the FAC.

ARGUMENT

I. Plaintiff's UCL allegations have not materially changed.

A. Plaintiff still claims only a "lost profit opportunity" for which he cannot recover under the UCL.

This Court held in June that Plaintiff had not alleged facts supporting a claim for restitution, the only monetary relief available under the UCL, because he did not seek to recover money in which he previously had any vested ownership interest. *Gonzales*, 2018 WL 3068248, at *2. Plaintiff's allegation that Uber's program "decreased the effectiveness of the Lyft app," harming Lyft and, in turn, Plaintiff and the other class members," was an allegation of a "lost profit opportunity." *Id*. Such an allegation is "one of classic money damages, not restitution." *Id*.

None of Plaintiff's amendments change this. He has added several allegations that Uber's goal was "to gain an unfair advantage in the market" or an "unfair competitive advantage" at his expense. SAC ¶¶ 1, 9, 11, 41. It did this by "diverting dual-app drivers" to Uber, "decreasing the availability of Lyft drivers," deterring riders from using Lyft and in turn harming Plaintiff. *Id*. ¶ 155. This supposedly led to "decreased overall earnings, decreased earnings per fare, cancelled fares, and a decrease in the quantity of fares per shift." *Id*. ¶ 10; *see id*. ¶ 11 (alleging Uber "manipulat[ed] ... the fare amount that [was] collected in the market place."). But these are the same allegations as before, asserting a claim for lost profits. This fails for reasons the Court has already explained.

Nor do Plaintiff's new "Prime Time" allegations change anything. SAC ¶¶ 101–06, 125. Plaintiff alleges that Lyft and Uber operate "incentive programs" that increase fares when demand is

high. *Id.* ¶¶ 102–03. He then alleges, "upon information and belief," that "in combination of [*sic*] Uber's fake rider accounts affecting Lyft's 'Prime Time' pricing scheme and implementing its own 'Surge Pricing' scheme, Uber can manipulate the market and affect fares collected by the Plaintiff and Class." *Id.* ¶¶ 104. To the extent this is a claim that Uber's "market manipulation" decreased Lyft's and/or Plaintiff's earnings during "Prime Time," Plaintiff again is making the same allegations as before—just that it happened at a different time of day. That hardly changes the nature of the claim, which Plaintiff concedes is one for "lost economic opportunities." *Id.* ¶ 105.

To the extent Plaintiff is claiming that, either during "Prime Time" or otherwise, Uber caused Lyft drivers like him to spend time and money "'chas[ing]' after non-existent fares" (SAC ¶ 101), or similarly that riders cancelled after he had already started driving toward them, that still does not change anything. For one thing, it is nothing but speculation. Plaintiff asserts that "it is plausible that those cancellations were the result of the proximity and convenience of Uber drivers as a direct result of Defendants' surreptitious conduct." *Id.* ¶ 105. But it is at least equally possible that the rider just decided not to travel at all, that a friend had also arranged a ride and so one of the two had to be cancelled, that another Uber *or Lyft* driver was nearby and/or more convenient as a result of chance and not the "surreptitious conduct," and so forth. But it makes no difference, because even if Plaintiff were not speculating about the cause, this would again be a classic money damages claim. He cannot recover damages under the UCL.

Thus, the SAC contains nothing new in terms of allegations for UCL monetary relief, only different words to describe the same theory. As the Court has already held, these allegations do not describe a viable claim for restitution.

B. Alleging that "Plaintiff *may* work for Lyft in the future" does not state a claim for prospective injunctive relief.

Plaintiff has put even less effort into the amended UCL injunctive-relief claim. In its June 21 order, the Court dismissed that claim because (1) Plaintiff had not alleged facts plausibly suggesting he could be harmed by the alleged retention of data about his location over three years ago, and (2) even if Uber were to restart the program, that could not harm Plaintiff because he no longer drives for Lyft and "has not alleged a desire to drive for Lyft in the future...." *Gonzales*, 2018 WL 3068248,

at *2 (distinguishing *Davidson v. Kimberly-Clark Corp.*, 889 F.3d 956 (9th Cir. 2018)). The SAC does not fix either deficiency.

First, Plaintiff has added to the UCL claim a single paragraph stating that injunctive relief is necessary because Uber "has not destroyed the wrongfully obtained data concerning the personal and private movements of Plaintiff ... such that injunctive relief is necessary...." SAC ¶ 152. Again there are no supporting facts. Plaintiff makes no effort to explain how this more than three-year-old data would pose any risk to him now, simply repeating an argument the Court has already rejected.

Second, Plaintiff also still has not alleged a desire to drive for Lyft in the future. He alleges only that he "*may* work for Lyft in the future." SAC ¶ 21 (emphasis added). That isn't good enough even under *Davidson*. *See, e.g., Lanovaz v. Twinings N. Am.*, 726 F. App'x 590 (9th Cir. June 6, 2018) (applying *Davidson*; holding allegation that plaintiff "would 'consider buying'" product was not enough); *Rugg v. Johnson & Johnson*, 2018 WL 3023493, at *7 (N.D. Cal. June 18, 2018) (also rejecting "would consider" allegation).

Even if Gonzales had alleged that he "intends to" work for Lyft in the future, that would still not have been good enough without supporting facts, which he does not provide. "Such 'some day' intentions—without any description of concrete plans or indeed any specification of *when* the some day will be—do not support a finding of the 'actual or imminent' injury that our cases require." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 565 (1992) (emphasis original). "Imminent" is an elastic term, but "it has been stretched beyond the breaking point when, as here, the plaintiff alleges only an injury at some indefinite future time, and the acts necessary to make the injury happen are at least partly within the plaintiff's own control." *Id.* at 565 n.2. A "mere profession of ... intent" is therefore not enough. *Id*. *Davidson* stretched the standing requirement about as far as it will go, but could not have stretched it further than *Lujan* allows. Gonzales's claim would fail, therefore, even if he *had* actually alleged an intent to drive for Lyft in the future. *See, e.g., Levay v. AARP, Inc.*, No. 17-09041 DDP (PLAx), 2018 WL 3425014, at *3 (C.D. Cal. 2018) (applying *Davidson* and citing *Lujan*; holding that "a bare allegation of intent to purchase will not do."); *Beckman v. Wal-Mart Stores, Inc.*, 2018 WL 2717659, at *3 (S.D. Cal. June 5, 2018) (dismissing because plaintiff did not

allege facts necessary to support *Davidson* argument). But he hasn't. He alleges only that he *may*, and that does not state a claim.

II. The Stored Communications Act claim fails.

"The SCA is not a catch-all statute designed to protect the privacy of stored communications; instead, it is narrowly tailored to provide a set of Fourth Amendment-like protections for computer networks." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004). Here too, Plaintiff's amendments have not fixed the problem the Court previously identified, and his interpretation of the SCA goes well beyond what this narrow statute was intended to protect.

A. Plaintiff has not alleged facts showing Lyft stored his data for "purposes of backup protection."

The Court dismissed Plaintiff's SCA claim because he had not alleged facts plausibly suggesting that the "communications" were "in electronic storage." *Gonzales*, 305 F. Supp. 3d at 1087. Under the SCA, that requires either temporary storage incidental to transmission (18 U.S.C. § 2510(17)(A)) or storage "for purposes of backup protection" (18 U.S.C. § 2510(17)(B)). Plaintiff no longer alleges the former, which, as the Court recognized, contradicts his claim that Lyft and Uber store geolocation data permanently. 305 F. Supp. 3d at 1087. Instead, he argues the "communications at issue" were stored by Lyft for "backup purposes" because it might retrieve them later "in response to, among other things, insurance inquiries, driver review, or valid subpoenas or other government requests." SAC ¶ 58 (citing Lyft Privacy Policy § 2(B));[2] *see also id.* at ¶¶ 113 (alleging data is backed up "for, *inter alia*, liability purposes."), 133 (alleging it may be used "to respond to government inquiries, insurance evaluations, or analyses of individual drivers, *inter alia*."). But while Plaintiff has thought up some purposes for which Lyft might have used the data, he still alleges no facts showing that any of those purposes qualify as being "for backup protection."

First, there have to be at least two copies of something for one to serve as a "backup." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004). In *Theofel*, the court held that copies of

[2] Lyft's privacy policy identifies a great deal of data that Lyft may collect, but says almost nothing about storage or use of the data about which Plaintiff is concerned here.

opened emails that remain on an email server could be deemed "backups" because they would provide a second copy of the message if the user accidentally erases a copy on the user's own computer.[3] *Id*. at 1075–76. But that would only be true, the court noted, for the kind of email service in which users actually download emails from the ISP's server to their own computer, as opposed to the (now more common) "web-based" email services where the only copy remains on the server. *Id*. As other courts have recognized, it follows from this (and the definition of "backup") that there must have been at least two copies of the relevant communications. *See, e.g. Anzaldua v. Ne. Ambulance & Fire Prot. Dist.*, 793 F.3d 822, 842 (8th Cir. 2015) (applying *Theofel* and holding subsection (B) did not apply); *Cline v. Reetz-Laiolo*, No. 3:17-cv-06866/06867-WHO, 2018 WL 3159248, at *28 (N.D. Cal. June 28, 2018) (same); *Flagg v. City of Detroit*, 252 F.R.D. 346, 362–63 (E.D. Mich. 2008) (same). Here, Plaintiff does not allege *he* was preserving any of the relevant data, or even that he could have, only that *Lyft* kept what it collected. Because Plaintiff does not allege he had a copy, or that Lyft had more than one, he does not allege the data Lyft was storing was a "backup."

Second, "[t]he mere fact that a copy *could* serve as a backup does not mean it is stored for that purpose." *Theofel*, 359 F.3d at 1076. For example, the Ninth Circuit noted, "[w]e see many instances where an ISP could hold messages not in electronic storage [as defined by the SCA]—for example, e-mail sent to or from the ISP's staff, or messages a user has flagged for deletion from the server. In both cases, the messages are not in temporary, intermediate storage, nor are they kept for any backup purpose." *Id*. Similarly, a business might (and virtually all do) keep copies of communications or other data for any number of business purposes, but under the SCA, at least, accessing copies kept for *those* purposes would not be a violation. In one similar case, for example, a plaintiff claimed that fleet tracking data—which included VIN numbers, driver names, and geolocation data—were being stored "for backup purposes" among others because users could view historical as well as contemporaneous data. *Cobra Pipeline Co. v. Gas Nat., Inc.*, 132 F. Supp. 3d 945, 948, 952 (N.D. Ohio 2015). But the court held it made no difference because the defendant had not actually accessed backup copies:

[3] This is the common understanding of "backup protection"—saving a second copy in case data is inadvertently deleted.

> Here Plaintiff identifies the weakness in its own argument. The information at SageQuest may have "also" been stored for backup purposes. But Defendant did not access these copies while they were "also" being stored for backup purposes. Instead, the Defendant accessed the primary means for accessing the data: the user-facing web portal. Any data viewed through that web portal was not being kept as a back-up. Merely because the data presented on the website included historical information does not render the website a means of storage covered under Subsection (B).

Cobra Pipeline, 132 F. Supp. 3d at 952.

Almost every case to consider the meaning of "backup protection" has involved email, reflecting the primary purpose of the SCA. This case does not. But no case holds that data (emails or otherwise) retained for business purposes like those Plaintiff has identified here (insurance, analytics, litigation, or investigation) are necessarily deemed stored "for purposes of backup protection." *See Noel v. Hall*, 525 F. App'x 633 (9th Cir. 2013) (holding defendant who stored communications for his own use was not doing so "as part of any 'backup protection' incident to providing communications service."). Almost any data could conceivably have some later use, but storing it for that reason does not make it a "backup" for SCA purposes.

B. Plaintiff does not allege Lyft acts as an "electronic communication service."

Additionally, the SCA is intended to protect communications being sent through "an electronic communication *service*," defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications...." 18 U.S.C. § 2701(a) (emphasis added); 18 U.S.C. § 2510(15). Plaintiff alleges only that Lyft's servers themselves are part of an "electronic communications *system*," which means facilities for transmission or storage of electronic communications. SAC ¶ 56; 18 U.S.C. § 2510(14). That is not enough.

Although Lyft certainly provides a service that *depends* on electronic communications, that is very different from acting as an "electronic communications service" (ECS) provider. Again, the statute is a narrow one, enacted with email and internet service providers in mind. *See generally* Kerr, *User's Guide to the SCA*, 72 Geo. Wash. L. Rev. at 1209–18. Just because a business uses the internet or stores electronic communications in the course of its business does not make it an ECS provider. One court reached that conclusion as to JetBlue, which also provides transportation services. *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 307 (E.D.N.Y. 2005). Amazon also is not an ECS provider for purposes of the Act. *Crowley v. CyberSource Corp.*, 166 F.

Supp. 2d 1263, 1270 (N.D. Cal. 2001). Neither is Lyft. *See also, e.g.*, *Hately v. Watts*, 309 F. Supp. 3d 407 (E.D. Va. 2018); *Keithly v. Intelius Inc.*, 764 F. Supp. 2d 1257, 1271–72 (W.D. Wash. 2011), *on reconsideration*, No. C09-1485RSL, 2011 WL 2790471 (W.D. Wash. May 17, 2011). Again, therefore, Plaintiff is trying to expand coverage of a narrow statute to cover something it was not intended to cover. For that reason as well, therefore, the Court should dismiss the SCA claim.[4]

III. Plaintiff's claim under the California Data Access and Fraud Act also fails.

The Court dismissed Plaintiff's CDAFA claim because he offered only "boilerplate" allegations parroting the language of five of the statute's subsections, with no supporting facts, leaving the Court and Uber to guess what his theory might have been. *Gonzales*, 305 F. Supp. 3d at 1090–91. The amended version of the claim is little better. SAC ¶¶ 137–43. Plaintiff now alleges that Uber "accessed information stored in Lyft's service" without permission (*id.* ¶¶ 140–41), and that "such conduct" violated "numerous provisions of the CDAFA including, but not limited to," subsections (c)(1), (2), and (7). *Id.* ¶ 142. Those subsections do not even use the terms "information" or "service," however, and Plaintiff does not explain how his allegations fit. As the Court has already held, Rule 8 does not allow complaints that require guesswork, and this one still does. As discussed below, however, the claims Plaintiff appears to be making would fail in any event.

A. Plaintiff does not allege Uber accessed *his* computer, computer system, or computer network.

In its previous order, the Court pointed out that under CDAFA, only the "owner or lessee of the computer, computer system, computer network, computer program, or data" may bring a civil action. 305 F. Supp. 3d at 1090 (citing Cal. Penal Code § 502(e)(1)). Because Plaintiff had not alleged "that Uber accessed *Plaintiff's* computer, computer system, etc.," the claim failed. *Id.*

Plaintiff now alleges only that Uber "accessed information stored *in Lyft's service*...." SAC ¶ 140 (emphasis added). He may have meant "Lyft's *servers*," but regardless he has again failed to

[4] The SCA claim also fails because the stored data were not "electronic communications," a term that expressly *excludes* "any communication from a tracking device." 18 U.S.C. § 2510(12)(C); *see In re App. of U.S. for an Order Authorizing Disclosure of Location Information*, 849 F. Supp. 2d 526, 577 (D. Md. 2011) (collecting cases holding smartphones qualify as "tracking devices" for this purpose). Uber previously made this argument (which the Court did not reach) as to the Wiretap Act claim. Doc. 38 at 11:16–12:4. The SCA incorporates the same definitions. 18 U.S.C. § 2711(1).

allege that Uber accessed a computer, system, or network that belonged to *him*. That means, at a minimum, that his (c)(7) claim should be dismissed, because that applies only to accessing a "computer, computer system, or computer network." Cal. Penal Code § 502(c)(7). Plaintiff has not explained how Uber violated this subsection in any event. *See* SAC ¶ 142 (describing (c)(7) as applying to "providing the [or "a"] means of accessing [a] computer system without permission...."). But he does not allege it did so by accessing a computer, system, or network that belonged to *him*.

What he appears to be alleging instead is that Uber violated subsection (c)(1) or (2) by accessing "his" *data*. *See* SAC ¶ 143 (alleging that Plaintiff is entitled to seek relief "[a]s owner of his personal data which Defendants accessed...."). Unlike (c)(7), those subsections do include the word "data." It is unclear, however, whether this statute allows a civil action by someone whose data was accessed while it was on someone else's computer. *See Cline*, 2018 WL 3159248, at *33 (suggesting the similar CFAA would apply only to physical or remote access of *the victim's* computer"; emphasis original). The Court need not reach that question here, however, because Plaintiff has not alleged facts showing that he actually owned the data Uber supposedly accessed.

B. Plaintiff does not allege Uber accessed *his* data, as opposed to Lyft's.

Plaintiff was not the "owner" of the data Uber accessed—Lyft was. No CDAFA cases have addressed the "ownership" of data in any detail, but Judge Alsup has held in one case that it was enough for the plaintiff to allege he "own[ed] the data *contained* in his email accounts." *Yee v. Lin*, No. C 12–02474 WHA, 2012 WL 4343778, at *3 (N.D. Cal. Sept. 20, 2012) (addressing claim that defendant took personal, business, and privileged information from plaintiff's emails; emphasis added). That suggests the distinction would be similar to that made in other contexts between the "contents" of a communication (which are protected) and associated "record" information (which is not). *See Gonzales*, 305 F. Supp. 3d at 1084–85 (dismissing Wiretap Act claim partly for this reason; citing *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014)); *see also id.* at 1091 (discussing constitutional claim; stating that Plaintiff offered "no authority to support his argument that the other information Uber allegedly obtained is generally considered private—Lyft ID number, working as a Lyft driver, and full names. The Court concludes it is not."); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1082 (N.D. Cal. 2015) ("[t]he geographic location of a mobile device at any given

time has likewise been deemed to be non-content information."); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) (holding geolocation data is generated automatically and so is not "content"). That, plus common sense, shows that Plaintiff is not the "owner" of the data for CDAFA purposes.

To begin with, Plaintiff does not explain his theory of "ownership" except to assert that under "Lyft's Terms of Service/Privacy Policy, the data is licensed to Lyft, but drivers like Plaintiff and Class members retain full ownership of their own personal data." SAC ¶ 5. Plaintiff does not cite the provisions on which this is based, but Lyft's terms hardly support the view that he retained "full ownership" of all personal data he shared with Lyft. *See* Lyft Terms of Service, Section 7 ("Your Information") https://www.lyft.com/terms/preview (last visited July 26, 2018). The TOS does *say* drivers "retain full ownership" of data—but that is "subject to the rights granted to [Lyft] in this Agreement," which include a "non-exclusive, worldwide, perpetual, irrevocable, royalty-free, transferable, sub-licensable (through multiple tiers) right" to use it as Lyft sees fit. *Id*. The Privacy Policy also shows that Lyft collected a great deal of information, personal and otherwise, from its drivers, and likewise expressly reserved the right to use it and share it with third parties. *See* Lyft Privacy Policy, https://www.lyft.com/privacy (last visited July 26, 2018). If property is the right to exclude others, then it is hard to see how Plaintiff "owned" any of this information under his agreement with Lyft (assuming a private contract controlled the application of CDAFA) in any sense that would give him a right to seek damages for copying it.

Beyond that, Plaintiff does not make clear what "personal data" he "owned." He could be said to own his name (though he is surely not the only "Michael Gonzales"), but he does not even allege his name (or home address) was among the data Uber allegedly got from Lyft. He must show he is "the owner or lessee of the computer, computer system, computer network, computer program, or data" *that was accessed*. Cal. Penal Code § 502(e)(1). Plaintiff does not allege Uber accessed his name or address—he speculates that it used data it accessed from Lyft to *determine* those things. *See* SAC ¶ 100 (alleging that Uber "used the data collected ... with other databases to learn personal details about Lyft drivers including, but not limited to, the drivers' full names [and] home addresses..."). Further, even if he owns his name, he has no privacy interest in it (*Gonzales*, 305 F.

Supp. 3d at 1091), and can hardly allege he was "injured" by its disclosure. Plaintiff has also added references to his license plate number and other "vehicle information." SAC ¶¶ 80–81. He does not explain why he owns those, if he claims to. If anyone "owns" his license plate number, it's the State of California. In any event, this is all information that he voluntarily gave to Lyft. At a minimum, once Lyft combined it with additional information, it became Lyft's, not Plaintiff's. *See United States v. Miller*, 425 U.S. 435, 440 (1976) (rejecting Fourth Amendment challenge to search of banking records because though records contained personal information, defendant "could assert neither ownership nor possession"; they were "business records of the banks").

Plaintiff also does not explain why he could be said to "own" data that Lyft or other people created or generated. Lyft created and assigned his Lyft ID number (just as the State created and assigned his license plate number). Lyft and Plaintiff's riders collectively generated his "driver rating." SAC ¶ 80. And his geolocation data was generated automatically. While it and other record data might accompany personal data he owns, just as in the Wiretap Act context that does not mean the record data *belongs* to him or that he has a protected interest in it. *See Yee*, 2012 WL 4343778, at *3 (suggesting plaintiff owned the contents of his emails); *Gonzales*, 305 F. Supp. 3d at 1084–85 (holding geolocation data is not "content"); *In re Carrier IQ*, 78 F. Supp. 3d at 1082 (same); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1061 (same). In short, if anyone owned the data Uber allegedly accessed from Lyft's "service," it would have been Lyft. But as Defendant and this Court have previously noted, Lyft is not here, and Plaintiff cannot assert a claim on its behalf.

C. Plaintiff fails to allege that Uber "circumvented technical or code-based barriers" as required under CDAFA.

All the relevant subsections require a showing that access was knowing and "without permission." Cal. Penal Code §§ 502(c)(1), (2), (7). In his CDAFA claim, Plaintiff alleges only that Uber's access was "was without permission, contrary to the Lyft Terms of Service, and surreptitious in that the spyware was not detectable...." SAC ¶ 141. This again fails to state a claim.

First, alleging that "terms of service" were violated is not enough. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016) (citing *United States v. Nosal*, 676 F.3d 854, 862–63 (9th Cir. 2012) (en banc)). In those cases, saying it was wary of creating sweeping potential

criminal liability for violating terms of service that are often vague and can be changed without warning, the Ninth Circuit construed the statutes at issue narrowly. *Id*. at 1066–69 (construing Computer Fraud and Abuse Act as well as CDAFA); *see also Oracle USA, Inc. v. Rimini Street, Inc.*, 879 F.3d 948, 962 (9th Cir. 2018) (also construing CDAFA narrowly). Plaintiff cannot base a CDAFA claim on the allegation that Uber violated Lyft's terms of service.

Second, consistent with CDAFA's purpose as an "anti-hacking" statute, most district courts have interpreted the "without permission" requirement to mean that a defendant must act "in a manner that circumvents technical or code-based barriers that a computer network or website administrator erects" to restrict or bar a user's access. *Facebook, Inc. v. Power Ventures, Inc.*, No. 08-cv-05780-JW, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010); *see also, e.g.*, *In re Google Android Consumer Privacy Litig.*, No. 11–mc–02264–JSW, 2013 WL 1283236, at *12 (N.D. Cal. Mar. 26, 2013) (holding use of tracking codes to collect personal data from Android phones was insufficient); *In re iPhone Application Litig.*, No. 11–md–02250–LHK, 2011 WL 4403963, at *12–13 (N.D. Cal. Sept. 20, 2011) (similar holding). At least one court has disagreed (*In re Carrier IQ*, 78 F. Supp. 3d at 1098–1101), but that is inconsistent with not only the majority view but also the Ninth Circuit's practice of construing these criminal statutes narrowly. *See also hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1107–1114, 1114 n.3 (N.D. Cal. 2017) (finding "serious questions" exist about strict application of CFAA or CDAFA to use of information from sites generally available to the public).

As before, though Plaintiff frequently uses buzzwords like "spyware" or "hacking," he actually alleges only that Uber created Lyft accounts—something anyone can do just by choosing a username and password—and then used open-source or commercially available traffic logging software to collect data sent to Uber by Lyft's servers. The SAC again does not allege, therefore, that Uber "circumvented any technical or code-based barriers" Lyft had erected, and so the CDAFA claim would fail for that reason as well.

D. Plaintiff fails to allege any "damage or loss."

Section 502(e)(1) refers only to compensatory damages for "expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network,

computer program, or data was or was not altered, damaged, or deleted by the access." Plaintiff does not allege anything of the kind. Nor could he, because as discussed above he did not own any of the listed items—Lyft did. In his CDAFA claim, Plaintiff makes no effort to explain what compensatory damages he might be entitled to "as owner of his personal data." SAC ¶ 143. *See In re Google Android Consumer Privacy Litig.*, at *11 (dismissing CDAFA claim because allegations regarding diminished value of personally identifiable information were not sufficient to allege damage or loss). Beyond that, Plaintiff's theory of economic loss in general continues to be based only on speculation. He still can only theorize that, "over time," Uber's actions might have "reduce[d] the effectiveness of the Lyft app" or otherwise affected the market, harming Lyft and in turn drivers "such as Plaintiff." Plaintiff has never supported this with any concrete facts, not even alleging, for example, that Lyft's ridership or income, or his own earnings, actually decreased while Uber's program was operating, or that they increased after it ended. Even if CDAFA permits damage claims beyond expenditures necessary to respond to a "hack," Plaintiff has not alleged claims for economic loss that are supported by anything but speculation. For that reason, too, his CDAFA claim should be dismissed.

IV. *Carpenter*'s narrow Fourth Amendment holding does not support Plaintiff's claim under the California state constitution.

In its April 18 order, the Court dismissed Plaintiff's invasion-of-privacy claims under the California Constitution, finding he had failed to adequately allege any of the three required elements: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct that amounts to a serious invasion of the protected privacy interest. *Gonzales*, 305 F. Supp. 3d at 1091–93 (citing *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35–37 (1994). That is still the case.

A. Plaintiff still alleges no legally protected privacy interest.

The Court previously held that Plaintiff had pleaded a protected privacy interest in home addresses and "arguably precise geolocation data," but held otherwise as to data such as his Lyft ID

number, details of his work for Lyft, and his full name.[5] *Id.* at 1091. Plaintiff offered no authority to show that this information is generally considered private, and "[t]he Court concludes it is not." *Id.*

Plaintiff has not addressed this in the SAC. The amendments focus almost exclusively on the "reasonable expectation of privacy" test (discussed below), and the amended cause of action is still unclear as to the scope of the "protected privacy interest" Plaintiff is claiming. Just as in the FAC, the closest the SAC comes to addressing this element directly is to assert that "Plaintiff and Class Members had a reasonable expectation of privacy as to *the interests invaded*." FAC ¶ 143, SAC ¶ 163 (emphasis added). Plaintiff's list of data types is now slightly different, but not materially so. He has added references to his "first name, type of vehicle driven, [and] license plate number," as well as his "driver rating" and "physical appearance" (SAC ¶¶ 79, 165), but it is hard to see how he could have a protected privacy interest in any of that. He also, of course, mentions his Lyft ID number (or "static identification number"), which he must include because it is central to his theory of the case—knowing that number is how Plaintiff claims Uber was able to track specific drivers who were using both apps. *Id.* ¶¶ 170–71. But again, the Court has already held that he does not have a protected privacy interest at all in his Lyft ID number, or in the details of his work for Lyft (or his full name). *Gonzales*, 305 F. Supp. 3d at 1091.

As for his home address, Plaintiff has yet to explain exactly how he believes Uber could have determined his home address—or, for that matter, why it would have wanted to—but he seems to be arguing that at least over time, Uber might have been able to deduce where he lived by observing where he most often switched on the app. *See* Opp. to Mtn. to Dismiss FAC at 22:16–18 (citing FAC ¶¶ 72, 83, 92); *see also* SAC ¶¶ 88, 99, 115 (the corresponding paragraphs). "For example," Plaintiff again alleges, if "Lyft driver[s] activated the app while still in the driveways of their homes, the Hell spyware would provide Uber with the means to discern where Lyft drivers lived." SAC ¶ 115. But Plaintiff never alleges *he* did this even once, only that "Lyft drivers" might have. For that matter, he

[5] Plaintiff actually did not allege that his Lyft ID number was accompanied by his name, nor did he explain how Uber might have determined his name or any class member's name from the anonymized data it allegedly collected. Uber pointed this out in its previous motion, and Plaintiff did not respond. Mtn to Dismiss FAC at 20:3–11. Notably, Plaintiff now alleges only that Uber could determine a *first* name (SAC ¶ 167), but again he does not explain how it might have done that, or what use Uber could have made of the extremely common first name "Michael."

does not allege he ever had his own driveway or a single-family home to go with it, things that in the Bay Area can hardly be assumed. If he lived in an apartment building, for example, knowing where he switched on the app would not identify him as an individual even if he *always* switched it on in the same place. In short, it is pure speculation on Plaintiff's part to suggest that Uber could have determined his home address, even assuming it had some reason to do that.

That leaves the alleged collection of large quantities of "arguably precise geolocation data," which at this point is the main thrust of Plaintiff's complaint. Plaintiff contends that *Carpenter* establishes that he has a reasonable expectation of privacy in his movements over time because of the "intimate" details those movements might reveal. SAC ¶¶ 161–74. But as discussed next, the question here is whether Plaintiff had a reasonable expectation of privacy in geolocation data *under the circumstances*, and the circumstances here are very different.

B. Plaintiff had no reasonable expectation of privacy under the circumstances.

1. *Carpenter v. United States*

Carpenter was a criminal case in which the defendant was convicted based on cell-site location information (CSLI) that placed him, or at least his phone, near the location of four bank robberies at the time they were being committed. 138 S. Ct. 2206, 2212 (2018). He moved to suppress that evidence because it had been obtained without a warrant, but the lower courts held he had no reasonable expectation of privacy in the information for Fourth Amendment purposes because it was information he had shared with third parties (his wireless carriers). *Id.* at 2212–13. The government therefore did not need a warrant because the collection did not constitute a "search." *Id*. In a narrow 5-4 decision, the Supreme Court reversed.

The majority emphasized the main purpose of the Fourth Amendment, namely to "safeguard the privacy and security of individuals against arbitrary invasions by *governmental officials*." *Id.* at 2213 (emphasis added; quoting *Camara v. Municipal Court of City & County of San Francisco*, 387 U.S. 523, 528 (1967)); *see also id*. at 2213–14 (repeatedly mentioning concerns about arbitrary government power and police surveillance). While sophisticated surveillance techniques may infringe on "a person's expectation of privacy in his physical location and movements," the majority noted, that had to be reconciled with the established principle that "a person has no legitimate

expectation of privacy in information he voluntarily turns over to third parties," even if turned over "on the assumption that it will be used only for a limited purpose." *Id*. at 2214–16 (citing *Smith v. Maryland*, 442 U.S. 735 (1979) (phone numbers called), and *United States v. Miller*, 425 U.S. 435 (1976) (banking records)). Under those circumstances, the majority noted, the Fourth Amendment offers no protection at all. *Id*. The question was whether to carve out an exception to that principle, and on the facts before it, the majority did so, holding that "when the *Government* accessed [cell-tower data] from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements." *Id*. at 2219 (emphasis added).

> By "the whole of his physical movements," the Court meant exactly that:
>
> > While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner *beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales*.... Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.
> >
> > * * *
> >
> > Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when.
> >
> > Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years [the length of wireless carriers' retention policies], and the *police* may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.

Carpenter at 2218 (emphasis added). The majority also found it important that not only are cell phones a "pervasive" and "indispensable" part of modern society, a cell phone "logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates [cell-site records].... As a result, in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements." *Id*. at 2220 (distinguishing *Smith*). The majority therefore held the third-party doctrine did not apply, and that the government's action was a "search" for Fourth Amendment purposes. *Id*. at 2221.

The majority emphasized the narrow scope of its decision:

> Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information.

Id. at 2220. The Court held only that the Fourth Amendment generally requires the government to get a warrant if it wants "unrestricted access to a wireless carrier's database of physical location information." *Id*. at 2223.

2. *Carpenter* does not change the result here.

As noted above, most of Plaintiff's amendments are an obvious attempt to bring his case within the holding of *Carpenter*. But again, as the Supreme Court itself emphasized, that holding was extremely narrow. It addressed only the Fourth Amendment and government surveillance. It addressed only the risk that the government might gain unrestricted access to the "whole of [a citizen's] physical movements." It did not address business records other than CSLI. And most importantly, it did not "disturb the application of *Smith* and *Miller*"—cases holding that *there is no reasonable expectation of privacy in records voluntarily turned over to a third party*. *Carpenter* at 2220. Because those cases remain binding, *Carpenter* is necessarily limited to its narrow facts—as more than one court has already held. *See Presley v. United States*, No. 17-10182, 2018 WL 3454487, at *4–5 (11th Cir. July 18, 2018); *Palmieri v. United States*, No. 16-5347, 2018 WL 3542634, at *6 (D.C. Cir. July 24, 2018); *Cohen v. Casper Sleep Inc.*, No. 17CV9325, 2018 WL 3392877, at *4 (S.D.N.Y. July 12, 2018).

In *Presley*, plaintiffs argued that *Carpenter* (and privacy protections in the state constitution) precluded the IRS from obtaining banking records without probable cause. 2018 WL 3454487, at *1–3. "[T]hat would be true," the court responded, "if Plaintiffs' clients had a reasonable expectation of privacy in the financial records held by the Bank." *Id.* at *4 (citing *Carpenter*). "But they don't."

> Rather, the third-party doctrine precludes that conclusion here. According to that doctrine, a party lacks a reasonable expectation of privacy under the Fourth Amendment in information "revealed to a third party and conveyed by [that third party] to Government authorities, even if the information is revealed on the

> assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."....
>
> In *Miller*, ... the Supreme Court considered whether a taxpayer enjoys a reasonable expectation of privacy in his bank records.... [It] rejected Miller's challenge for two reasons. First, Miller had "neither ownership nor possession" of the documents because they were "business records of the banks." Second, the nature of the records the IRS was seeking—checks—further limited Miller's expectations of privacy since the checks were "not confidential communications but negotiable instruments to be used in commercial transactions." The Supreme Court recently reaffirmed the vitality of *Miller*'s holding. *See Carpenter v. United States*, 138 S.Ct. at 2220 (2018) ("We do not disturb the application of ... *Miller*....").
>
> Both of the Supreme Court's considerations in *Miller* also apply here.... In short, *Miller* precludes us from holding that Plaintiffs' clients have a reasonable expectation of privacy in the summoned records.[6]

Id. (most citations omitted).

At least two other courts have similarly held that *Carpenter* does not apply beyond its narrow holding, like *Presley* specifically noting that the Court otherwise left the existing "third-party doctrine" undisturbed. *Cohen*, 2018 WL 3392877, at *4 (holding that despite *Carpenter*, Cohen may not contort Defendants' surreptitious conduct into an illegal wiretap claim where consent bars such claims."); *Palmieri*, 2018 WL 3542634, at *6 (holding defendant had no reasonable expectation of privacy in information shared with Facebook friends, even though defendant assumed it would not be shared; distinguishing *Carpenter*).

As these cases also demonstrate, nothing in *Carpenter* affects the principles this Court applied in finding that Plaintiff had not alleged a reasonable expectation of privacy in the information he shared with Lyft (among others). *Gonzales*, 305 F. Supp. 3d at 1091–92. He "consented to the sharing of his geolocation data with perfect strangers," and so under the circumstances he could not expect it to remain private. *Id*. at 1092. Even if he "toggled on" at home, and assuming Uber could actually determine his home address as a result, "under the circumstances drivers did not have a reasonable expectation of privacy in their home location." *Id*. Plaintiff's argument that his consent was limited to Lyft is still unavailing (*see id*.); as *Cohen* recognized, *Carpenter* does not change that aspect of the third-party doctrine. 2018 WL 3392877, at *4.

[6] Moreover, the court held that the Florida constitutional provision granting a privacy interest in bank records was preempted because it would substantially impede the federal government's interest in obtaining bank records as authorized by federal law. *Id*. (citing cases).

Even if *Carpenter* applied in cases like this one, the facts are simply not the same. Again, the Court's narrow holding concerned government tracking—without knowledge or consent—of "the whole of [one's] physical movements," not just those on public streets. "A cell phone faithfully follows its owner *beyond public thoroughfares* and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.... [W]hen the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." 138 S. Ct. at 2218 (emphasis added). Despite Plaintiff's best efforts in three complaints, he has alleged nothing remotely like this. He *consented* to have his location tracked. It was tracked only while he was logged into the Lyft app, and then only because he had chosen to use the Lyft app. Even Plaintiff's claim that Uber could determine his home address if he "toggled on" in his driveway is nothing but speculation.

Again, Plaintiff's theory is that Uber wanted to track Lyft drivers' IDs *while they were driving* so it could try to match those IDs with the locations of drivers it knew were using the Uber app, in order to entice those dual-app drivers to use the Uber app exclusively. He has never even articulated, much less pleaded facts to support, a theory as to why Uber might have been interested in tracking him or any other Lyft driver at any other time. And notably, Plaintiff has misquoted Lyft's privacy policy when he claims that the Lyft app may have tracked him even when it was off (and so, presumably, into "other potentially revealing locales"). Plaintiff alleges that "[s]uch information may even be collected when the application is turned off 'to identify promotions or service updates in your area.'" SAC ¶ 115 (quoting Lyft Privacy Policy § 2(B)). In fact, that sentence reads, "*If you give us permission through your device settings or Lyft App, we may collect your location while the app is off* to identify promotions or service updates in your area." Lyft Privacy Policy § 2(B) (second paragraph, emphasis added). Plaintiff has not alleged *he* gave Lyft permission to do that. If he did not, then presumably Lyft did not collect data while his app was off. If he did, his consent would mean he had no reasonable expectation of privacy in the result. *Miller*, 425 U.S. at 442; *see Carpenter*, 138 S. Ct. at 2220 ("We do not disturb the application of ... *Miller*....").

Therefore, *Carpenter* does not apply beyond its narrow holding, and even if it did Plaintiff has not alleged anything like the "near perfect," "tireless and absolute" government surveillance the

Supreme Court was concerned about in that case. For the reasons this Court has already stated, therefore, Plaintiff had no reasonable expectation of privacy in the information Uber allegedly collected, and that alone defeats his state constitutional claim.

C. Plaintiff's claim here would still fail because he has not alleged a violation sufficiently "serious" to violate the state constitution.

Finally, even setting aside the above, *Carpenter* does not change the fact that California requires "egregious" conduct resulting in a "serious" privacy violation before allowing a cause of action under its state constitutional provision. *See, e.g., In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 (dismissing claim because disclosure of plaintiffs' unique device ID number, personal data, and geolocation information did not constitute an egregious breach of social norms); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127–28 (N.D. Cal. 2008), *aff'd*, 380 Fed. App'x 689 (9th Cir. 2010) (holding that negligent conduct leading to theft of highly personal information including Social Security numbers did not "approach [the] standard" required by the California Constitution). As this Court noted, "[e]ven disclosure of very personal information" has been deemed insufficient to meet this high standard. *Gonzales*, 305 F. Supp. 3d at 1092 (quoting *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014); citing other cases). And as it recognized, even if Plaintiff's allegations that Uber obtained his name and home address were plausible, "[w]ithout more allegations as to what, if anything, Uber did with this information, Plaintiff has not plausibly alleged a serious invasion of privacy." *Id.* at 1093. Plaintiff has not even attempted to fix this in the SAC, much less alleged any facts making this claim any more plausible.

CONCLUSION

After a year and a half and three complaints, Plaintiff's allegations have not moved far from where they began: an online article cut-and-pasted into a pleading. Ironically, in a case alleging the compilation of an all-encompassing, "intimate" picture of the life of a Lyft driver, we still know almost nothing about Michael Gonzales. Nor has any other plaintiff come forward to allege a serious violation of fundamental privacy rights, or an economic loss as a result of Uber's alleged program. Nor has Lyft complained about the alleged effect on its business, from which Plaintiff's injury supposedly derives. Most of Plaintiff's new allegations are a last-ditch effort to argue that *Carpenter*

rescues his case. It does not. Because Plaintiff's SAC still does not fix the problems this Court identified in its previous orders, the Court should dismiss the case with prejudice.

Dated: August 1, 2018

Respectfully Submitted

SHOOK, HARDY & BACON L.L.P.

By: */s/ M. Kevin Underhill*
M. KEVIN UNDERHILL
ELIZABETH A. LEE

Attorneys for Defendants
UBER TECHNOLOGIES, INC.; UBER USA, LLC; and RASIER-CA